Strategy Research Project

CONSOLIDATING OUR COUNTRY'S BIOMETRIC RESOURCES AND THE POSSIBLE IMPLICATIONS

BY

COLONEL ELOY CAMPOS
United States Marine Corps Reserve

USAWC CLASS OF 2008

U.S. Army War College, Carlisle Barracks, PA 17013-5050

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 MAR 2008	**Strategy Research Project**	**00-00-2007 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Consolidating Our Country's Biometric Resources and the Possible Implications	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Eloy Campos	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College ,122 Forbes Ave.,Carlisle,PA,17013-5220	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**26**	

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

USAWC STRATEGY RESEARCH PROJECT

CONSOLIDATING OUR COUNTRY'S BIOMETRIC RESOURCES AND THE POSSIBLE IMPLICATIONS

by

Colonel Eloy Campos
United States Marine Corps Reserve

Colonel Michael Marra
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Eloy Campos

TITLE: Consolidating Our Country's Biometric Resources and the Possible Implications.

FORMAT: Strategy Research Project

DATE: 2 March 2008 WORD COUNT: 5,581 PAGES: 26

KEY TERMS: (Fingerprints, Retinal and Iris Scans, Interagency Consolidation, Signature Verification, Civil Military Responsibilities)

CLASSIFICATION: Unclassified

The events of September 11, 2001, set in motion a revolution in the field of security and security-related research. The use of biometrics for the purpose of ascertaining an individual's unique characteristics is not a new idea but the September 11, 2001, terrorist attacks upon the United States helped to propel the industry into the front lines of the Global War on Terrorism. Due to the great potential for the exposure of private, individual information to would be criminals, the industry and the government are now facing a myriad of questions regarding societal and ethical implications associated with the widespread use of this technology.

A CASE FOR CONSOLIDATION OF OUR COUNTRY'S BIOMETRIC RESOURCES AND THE POSSIBLE IMPLICATIONS

> To those champions who avowed the truth day and night… And wrote with their blood and sufferings these phrases…The confrontation that we are calling for with the apostate regimes does not know Socratic debates…, Platonic ideals…, nor Aristotelian diplomacy. But it knows the dialogue of bullets, the ideals of assassination, bombing, and destruction, and the diplomacy of the cannon and machine-gun. Islamic governments have never and will never be established through peaceful solutions and cooperative councils. They are established as they [always] have been, by pen and gun, by word and bullet, by tongue and teeth.
>
> —The Al-Qaeda Training Manual
>
> August 2004

Biometrics - Past and Present

"In the battle between good and evil science holds the balance of power. It's impossible to commit a crime without leaving a trail."[1] And it all started with Sherlock Holmes in 1880's England. The incredible ability of the fictional detective to solve crimes from the most negligible physical clues inspired an imaginary Scotland Yard to follow his lead and search for the trail of criminals in the physical evidence left behind at every crime scene. Unwittingly, this fictional character may have set in motion what is today the field of Forensic Sciences. Biometrics, a subfield of Forensic Science, focuses on the measurement of specific physical or behavioral characteristics and the use of those characteristics in identifying subjects.[2] Examples of such person specific data include retinal and iris scans, fingerprints, signature verification, hand geometry, facial features, DNA sampling, speech patterns, gait, and even body odor, just to name a few.

Accordingly, senior leaders at the US Department of Defense (DoD) have recognized that biometrics can be a potent weapon in prosecuting the Global War on

Terrorism. Today, Provincial Reconstruction Teams (PRTs) operating in Iraq and Afghanistan collect biometrics data to identify, categorize, and otherwise track movement of the populace within their respective areas of operation. During my tenure in Iraq where I was in charge of civil affairs activities in the city of Fallujah, we collected in excess of 250,000 retinal and fingerprint scans on the local populace. This data was then used to issue resident identification cards and to compare against a central database at Multi-National Forces West (MNFW), in order to check for known persons involved in the insurgency. On multiple occasions the resulting biometrics, fingerprints, and/or retinal patterns match led our forces to insurgents' homes and their centers of activity. On other occasions, we were able to recover remains of suicide bombers and run their data through the system and establish their identities; all that was needed was a finger or an eye.

Recognizing the enormous potential of this scientific advancement, the US Army has been designated by the US Congress as the lead agency for the development and implementation of biometrics technology across DoD. As a result of this charter, the US Army has established the Army Biometrics Task Force (BTF), recently renamed the Biometrics Fusion Center (BFC). This organization's main focus is to support the Global War on Terror, to secure DoD facilities and networks, to develop biometrics standards, and to initiate the implementation of these initiatives.[3] As the use of biometrics for purposes of identifying and classifying individuals takes hold in the United States, the issue of personal privacy will become even more sensitive. The American Civil Liberties Union believes the nascent biometrics industry will have to be regulated citing what it calls the "big brother" factor.[4] For those leaders in the industry this is of vital concern to

the American public as the access to this vast repository of personal information brings with it great responsibility.

A Case for Integrating our Country's Biometric Technology Systems

The global spread and easy access to sophisticated weapons grade technologies has been a key medium for America's enemies to coordinate and execute terrorist attacks against friendly governments. Al-Qaeda operatives in Iraq use cellular phones to remotely detonate bombs and employ Improvised Explosives Devices (IED) against Iraqi and coalition forces trying to bring stability to that war torn part of the region. The 9/11 highjackers made free use of the internet to send coded messages between each other. As plainly stated above, Osama bin Laden's ideals are powerful motivators for pro-Islamic radicals determined to destroy our democratic way of life. Through rhetoric, pen, word, and tongue, and through violence, gun, bullet, and lies, radical Islam is mobilizing its forces in what has proven to be an all out rejection of modernity and an armed assault on any nation state that stands in the way of a unified caliphate. Neither oceans nor borders will deter those elements from attempting entry into our county and wreaking havoc within our communities.

Individual Access Control Measures

Access control measures are actions taken to grant right of entry to restricted physical spaces or records or systems containing data that only authorized individuals are cleared to enter or access.[5] Three factor (3-factor) authentication protocols are quickly becoming the method of choice for high security systems in government as well as in Corporate America. [Three] 3-Factor authentication relies on verifying something a person has, such as a Common Access Card (CAC)/Smart card or token, something a

person knows, such as a password or Personal Identification Number (PIN), and something a person is, such as a measurable biometric, fingerprint, facial image, hand/palm scan, etc. As described above, a biometric characteristic is a measurable physiological and/or behavioral trait that can be used in an automated recognition system.[6] In discriminating the authenticity of an individual, different technologies or a combination of technologies may be employed. Scientists and engineers at our nation's leading research institutions continue to explore new techniques and develop useful mathematical algorithms that will make biometrics identification technology feasible, practical, and affordable to the government and Corporate America. Following is a discussion of five of the most promising technological developments that seek to incorporate the use of biometrics information into robust personal identification systems.

Fingerprint Technology

Fingerprints have been used to match individuals to recorded print images for decades. Fingerprints are widely accepted as being unique to each human being. "A fingerprint is a pattern of ridges and valleys on the surface of a fingertip whose formation is determined during the first seven months of fetal development."[7] The United States Federal Bureau of Investigation (FBI) maintains one of the world's largest and most complete databases of fingerprint information. While the agency has been successful at matching millions of prints to suspected criminals, the actual process of ascertaining a positive match is lengthy and cumbersome. In many instances authorities cannot hold a suspect pending a positive fingerprint match. As technology evolves and becomes faster, more robust systems are deployed. This will unquestionably be a useful tool in our nation's arsenal of terrorists-fighting measures. However, because the

FBI's systems do not currently fully interact with Department of Homeland Security (DHS) United States Visitor and Immigrant Status Indicator Technology (US-VISIT) systems, this compatibility issue could take several years to resolve.

Retina Scans

Biometrics technology that analyzes the complex and unique characteristics of the human eye can be divided into two different fields: iris biometrics and retina biometrics. An iris recognition system uses a video camera to capture the image while the software compares the resulting data against a stored, master template. Retina scans, on the other hand, are performed by directing a low intensity light into the eye to capture the unique characteristics of the human retina.[8] This data is then digitized and stored as a base template, much like a fingerprint, or any of the other biometrics characteristics of a human being. Iris scans are considered to be more accurate than retinal scans because the number of data points is much greater in the structure of the iris than it is in the retina. This technique, therefore, produces greater accuracy when matched against the master iris template. Retinal scan devices are the most accurate biometric available today. The continuity of the retinal pattern throughout a person's life, and the difficulty associated with deceiving such a device, also make it a great long-term, high-security option. As a result, retina scan security systems are used almost exclusively in high end security facilities such as nuclear power plants, advanced research installations, and the like.[9]

Facial Recognition

Facial recognition, much like retinal and iris scans, identifies individuals by analyzing the unique patterns and contours of an individual's facial features.[10] As in eye

scanning technology, there are two basic methods of analyzing facial features: video and thermal imaging. “Standard video techniques are based on facial images captured by a video camera. Thermal imaging techniques analyze the heat generated pattern of blood vessels underneath the skin.”[11] Law enforcement and security experts disagree on the utility versus the cost of facial recognition systems. Reliability data suggests some of the better facial recognition systems can have high rates of false matches, or similarly, high rates of no matches. These systems impose a number of environmental restrictions that require simple and well lit backgrounds, multiple angle shots, and a relatively close proximity to the capturing device in order to obtain sufficient contextual information to match the stored template.[12] Additional restrictions on facial imaging systems are factors influencing the fact that they can be easily altered by losing weight, wearing glasses, the way an individual combs his/her hair, and even by wearing a false mustache or a disguise. In the U.S., issues of privacy could surface since making a video of an individual’s face does not necessarily imply consent, thereby inviting the ire of privacy rights advocates.

Signature Verification

Signature verification is probably one of the oldest means used by humans to validate or confirm authenticity. However, also well known is the fact that signatures are one of the easiest methods used to falsify an individual’s identity. New signature recognition systems take these variables into account, however, and use the standard loops and hoops as one of the many data points used to establish the base template. Other unique signature elements such as spiral pressure, lettering strokes, and even the individual’s state of mind at the time of signing can be correlated and analyzed. A

reliable signature verification system includes means for obtaining data related to a given signature and means for comparing that data with various samples obtained previously.[13] While signatures over the ages have been used to ascertain individuals' authenticity, signatures are behavioral biometrics that change over time and are influenced by the emotional and physical conditions of the signatories.[14] Experts disagree, nevertheless, on the veracity of relying solely on a signature to validate a person's identity. However, when used in combination with other biometrics means, signature verification systems add another layer of security to a personal verification scheme.

Smart Cards

Smart cards are quickly making inroads into the US market after enjoying enormous success in Europe over the last 30 years. The first generations of smart cards are still in operation today and are well known as credit cards, or other cards containing magnetic strips on the back. Today's smart cards use an embedded microprocessor to store and retrieve information. The sophistication of that microprocessor, first perfected in Global System for Mobile Communications (GSM) cell phones in Europe, is exponentially better than the technology in magnetic strip media. The microprocessor technology essentially emulates that of a computer on a much smaller scale, obviously. The real advantage is that the tiny microprocessor is embedded inside the plastic medium in the card and the onboard storage is thousands of times greater than the old magnetic strips. The newest smart cards may contain upwards of 8 kilobytes (K) of Random Access Memory (RAM), 346K of Read Only Memory (ROM), 256K of programmable ROM, and a 16 bit microprocessor, and the

processor uses a limited instruction set for encryption of applications.[15] Thinking back to the mid-1940's, the reader will recall the first (artillery firing table) computer, the Electronic Numerical Integrator and Computer (ENIAC), stored data in punch cards, contained over 17,000 vacuum tubes, and occupied an entire room. As more modern miniaturization and data compression standards are integrated into smart card chips, the onboard storage capabilities and processing will continue to increase and access speeds will improve vastly. The advantage is that the amount of data storage will allow greater granularity of stored information. Depending on the application of the smart card, tens of thousands of individual data points may be stored. Already, many corporate and financial institutions store records of individuals' fingerprint data, retinal and/or iris images, and facial and other biometrics characteristics on microchips embedded in smart cards. Additionally, entire historical records such as an individual's medical history are being stored on smart card electrically erasable programmable read-only memory (EEPROM), or microchips. The medical industry also employs an encryption algorithm that protects the data with 128K encryption technology

The Transportation Security Administration (TSA) has begun to roll out a program called Fly Clear. The purpose of the Fly Clear program is to facilitate passenger's quick access through airport security by pre-clearing travelers. The Fly Clear smart cards store the passenger's personal information such as name, date of birth (DOB), address, passport numbers, etc., along with an image of the bearer's fingerprint and a scanned image scan of the iris. Once at the airport, the TSA attendant inserts the smart card into a reader and the passenger is asked for a fingerprint and iris counter sample images. One of the more significant advantages of the smart card technology is that verification

of biometrics data is performed locally, while the passenger is waiting to gain access to the terminal. The smart card reader decrypts the biometric data stored on the card's microchip and compares it to the sample provided by the passenger on the spot without the need to access a network or a master database at an offsite location. If the biometrics data on the card matches that of the individual requesting passage then he is allowed to enter the secured airport passenger areas.[16] This approach to ascertaining an individual's credentials is fast and convenient, and one of the most sophisticated and technologically advanced applications of biometrics technology today.

On a larger scale, this same technology could be used to screen visitors entering the country, or workers requesting access to secured locations in a host of industries and applications. Similarly, smart card chip sets could be used to verify a passenger's luggage count prior to boarding and after disembarking aircraft or other commercial vessels. This way, authorities would be assured that no malicious packages could be introduced or abandoned in passenger aircraft or vessels. At the time the passenger checks his luggage with a counter agent or at a check-in kiosk, he would be required to upload data to the storage chip on the smart card indicating his baggage count, destination, number of stops, delay en route, purpose of trip, and/or a host of other relevant information.

Biometrics proponents and civil rights activists differ on the practice of storing personal data into smart card chips. Many privacy and security related questions arise once this data is used for other purposes. Questions such as: Will the biometric data be used to track people covertly thereby violating their right to privacy?; Can the medical condition of an individual be surreptitiously elicited from the biometric data encoded in a

smart card?; Will the acquired biometric data be used only for the intended purpose, or will it be used for previously unexpressed functions, hence resulting in functionality creep?[17] These are all legitimate and important issues that must be addressed. As discussed later in this study, the availability and access to the population's personal information presents numerous challenges to the responsible agencies and its leaders. First and foremost, the citizens' confidence in the system must be guaranteed and leaders up and down the responsible government or civilian agency must be the ultimate guarantors of the public's confidence. In addition to leadership responsibilities, government regulations are also required in order to prevent the inappropriate transmission, exchange, or processing of citizens' biometric data.[18]

Challenges of Integrating Biometrics Technologies into a Single System

"The real meat of a modern Identity Management system is not the front end, badges, tokens, and/or biometrics, but the information system in which they operate, the "IT Backplane". Complex and expensive tokens such as smart cards are useful and prescribed in many applications but, if limited to local operation, are often impractical in situations where DoD seeks an ID solution."[19]

Today, almost every major government agency has its own method of storing and retrieving person-specific information for security purposes. The best known and by far the oldest and most successful is the FBI's Integrated Automated Fingerprint Identification System (IAFIS). This system, in existence since the early 1970s and maintained by the FBI's Justice Information Services Division, is the largest biometric database in the world and contains approximately 48 million templates in its master file; this database receives about 50,000 query searches a day from the various FBI offices

around the world. Even by today's standards, this system is an absolute technological marvel, even though it is over 30 years old. However, its biggest problem is its isolation and its incompatibility with other, newer, more technologically advanced identification systems. However, for all intents and purposes, this gargantuan database store is a legacy system. When compared to other government agency programs such as the DHS US-VISIT, DoD Automated Biometric Identification System (ABIS), and TSA Fly Clear, this system is already a relic of the past. Even more perplexing is the fact that, as of this writing, none of these advanced systems are interoperable with each other. Unrestrained, these government institutions will continue to develop, maintain, and resource dissimilar biometric systems that, independently, will not be able to close the gap on our nation's security infrastructure.

The US-VISIT program is a broader security system now deployed at 115 airports and 15 seaports around the country. Visitors wishing to visit the United States have their left and right index fingers scanned at the time they request a visa. In many cases, US-VISIT begins overseas at the U.S. consulate offices issuing visas, where visitors' biometrics are collected and checked against a database of known criminals and suspected terrorists. When the visitor arrives at the U.S. port of entry, the same biometric data is used to verify that the person requesting entry is the same person who received the visa. *(Incidentally, this could also be a criminal or terrorist whose biometrics data has not been collected; i.e. a terrorist who has not yet been caught.)* The resulting biometric data is then used to validate the individual's identity at the time of entry.[20] What these visitors don't realize is that by then their biometrics information has been analyzed by the US-VISIT central database to screen out potential terrorist

agents or identified political undesirables. The predicament with this system is that currently the US-VISIT program is not interoperable with either the FBI's IAFIS or DoD's ABIS. Thus, even if a potential terrorist overseas has been enrolled into ABIS or IAFIS, he could still obtain entry into the US because the US-VISIT database would not have visibility of the information available from the other two government agencies.

The DoD Biometrics Task Force (BTF) under the leadership of the Mr. Paul McHale has made great leaps towards implementing ABIS, the DoD Automated Biometric Identification System. This system, undergoing deployment as of this writing, is focused on serving DoD agencies on the forefront of the Global War on Terror (GWOT). As Mr. McHale points out, "our enemy today is no longer in uniform; our enemy today is probably wearing civilian clothes and is virtually indistinguishable from innocent…civilian counterparts in our society. Biometrics identification…is an important way to distinguish friend from foe."[21]

The BTF focus of effort is still on supporting DoD agencies but has also begun work to incorporate technologies in order to integrate other existing biometrics resources at our nation's disposal. The effort to connect DoD's ABIS to the FBI's IAFIS database is a significant step in that direction. And while this proposal is beginning to yield some benefits, the systems are still years away from being fully interoperable. For one reason, ABIS's enrollment data records only include fingerprint data points from an enrollee's left and right index fingers, while the FBI's database utilizes the enrollee's ten fingers. Neither of these two systems currently uses other biometrics data such as iris or retinal scans, signature verification, facial recognition, or even a picture of the enrollee. And while a picture of the enrollee is taken at the time of enrollment, that picture does

not become part of the biometrics profile of that individual. Given the recent technological advancements in data storage and compression, this is a significant shortfall in the process.

Other biometrics identification systems available and in use today such as DHS's US-VISIT and TSA's Fly Clear, are undeniably more technologically advanced than DoD's ABIS and the FBI's IAFIS. Of significance is the fact that US-VISIT uses the enrollee's ten fingers, iris scans, and a digital picture (the one found on the individual's passport). Additionally, enrollee's data such as date of birth, address, vital statistics, etc., are all available at the time his credentials are presented. Also of interest is the fact that when the individual's fingerprint and iris scans are taken at the point of entry, that data is immediately searched, matched, and presented to the customs agent for verification, instantly. In contrast, an FBI biometrics search takes over two hours to complete, whether a match exists or not. Finally, and to illustrate the vulnerability of the US-VISIT program, this system is only used to screen foreign visitors.

The Transportation Security Administration's Fly Clear program offers similar capabilities but is even more technologically sophisticated. And while deployment of this system is still in its infancy, it offers significant technological breakthroughs. This system uses smart card technology to store the enrollee's biometrics data, fingerprints, and iris scans. Upon arrival at the airport, the bearer hands his Fly Clear smart card to the agent. The agent inserts the card into the reader and obtains his data. To verify the enrollee's identity, his fingerprints and iris scans are taken and instantly compared to those stored in the microchip embedded in the smart card. A significant deficiency of this program is that it is only available to U.S. domestic passengers. Of note, the

Department of State (DOS) also has plans to transition to biometric imprinted passports for all U.S. passports. Currently, however, only U.S. Diplomatic passports contain the bearer's biometric data.

The Disconnect

As of this writing, none of these distinct government systems is able to completely interoperate with the other. And while the leaders of the DoD's ABIS and of the FBI's IAFIS are working to that end, we are still maintaining separate and isolated security systems -- well intentioned but lacking in cohesion and focus.

Connecting the nation's biometric databases of the FBI, DoD, DHS, and TSA makes practical and economic sense, not only in human resources but also in technological and capital investments. By searching these data records against all relevant databases, we will be able to link individuals with any known aliases or criminal activities.[22] The leadership within DOD and the FBI understand the flexibility and strength a networked system would bring to bear on the process of controlling access to U.S. borders and cities. Figure 1, below, depicts DoD's proposal to connect ABIS to the FBI's IAFIS; however, this proposal is only incremental and short-sighted. The objective should be a long-term focus of effort on a system of systems architecture where all appropriate government agencies have access to each other's resources, Figure 2. Corporate America, for instance, rid itself of stove piped systems long ago and has since moved towards a flattened architecture where distributed business units share corporate resources that are centralized geographically and logically. In this scenario a border patrol officer should be able to use a biometrics data cross reference against all government security agencies without that agent even having to know that is what he is

doing. Ideally, that agent should be able to obtain a person's biometrics data, fingerprint, iris, or retinal scan, etc., by pressing a terminal key at a border checkpoint, and that query should access the government's security databases and return a result within 30 – 45 seconds.

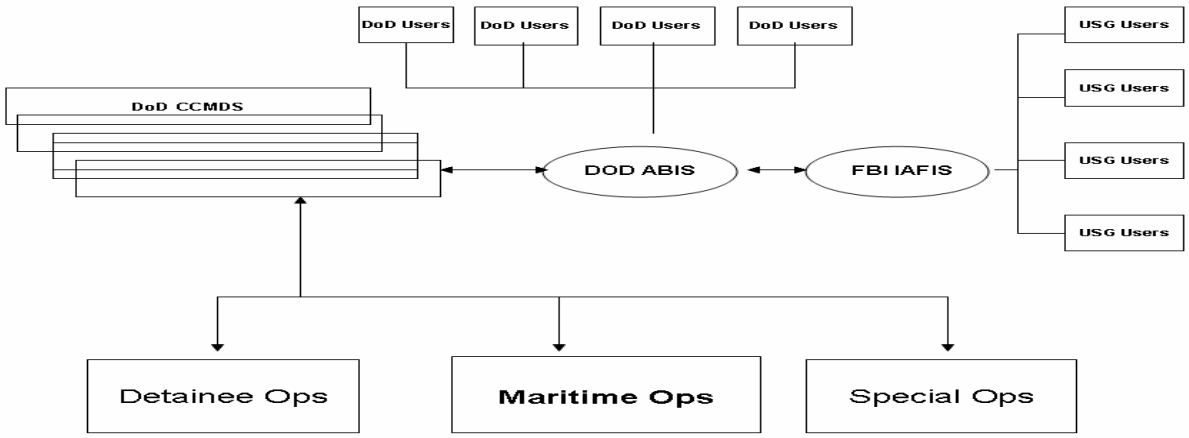

Figure 1: Proposed Migration of Existing System [23]

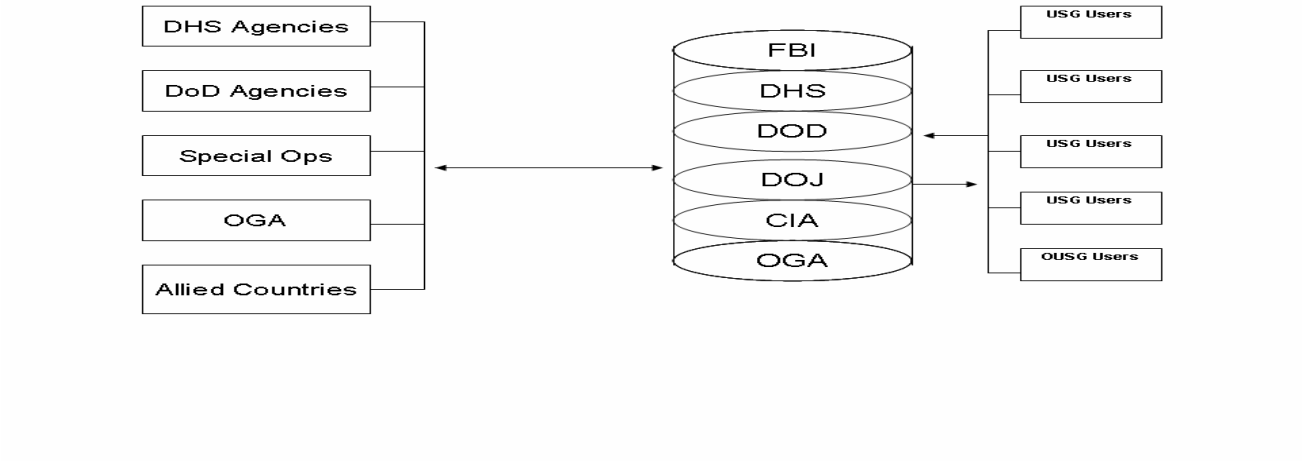

Figure 2: Recommended Integrated Biometrics System

The proposal diagram in Figure 2, above, depicts a system that would enable simultaneous access with a high degree of reliability and availability. This concept is known as distributed computing and is not a new idea. Companies such as Chiquita Brands International, Inc., and Johnson and Johnson, Inc. use similar systems today. These distributed databases are strategically positioned on locations around the globe and whether a user is in North America or some remote region of Australia, that database is accessible 24 hours a day, 7 days a week, year round. I mentioned above that the key to making this feasible is the information technology backbone or infrastructure. In fact, these infrastructures already exist and are operational today in Corporate America and throughout all government agencies. Correspondingly, robust global network connectivity is not the obstacle to implementation of a connected biometrics security system today.

Civil Military Implications

Because the management of biometrics information in this county for purposes of Homeland Defense has essentially become a military mission, the civil military implications will no doubt be daunting. Citizens' privacy concerns have already reached the desks of political leaders who are now pressuring the Army's BTF to find better ways to respond to the public's expectations of privacy, to shape those expectations to a prudent extent, and to take action against negative media exposure, which is not only embarrassing but can set back important policies, technologies, and systems.[24] The central issue in this debate is the challenge of identity management. The assumption is that the military is collecting this type of information and using it as a repository to track would-be criminals. But, as has been the case with social security and credit card

numbers, criminals can surreptitiously obtain this formation and duplicate an individual's identity for the benefit of their own perverted intentions. One can clearly establish the staggering implications of a determined hacker acquiring the source identities of even just a few dozen citizens. Once in possession of a person's means of identification, a criminal has instant access to that person's name, social security number, date of birth, address and telephone number, biometrics data, driver's license and access devices, bank and credit card numbers, and personal identification numbers, among others.[25] Recently publicized cases of identity theft reveal the devastating effects to families' lives and ruined careers of average American citizens.

Correspondingly, the fact that the government, specifically the military, will have complete control over this vast bank of personal information is enough to make the most trusting citizen apprehensive. While Americans still admire and respect their military, it would not take much to turn that love into odium and distrust. Just one incident of the military using this data to infringe on a person's right to privacy will precipitate the undoing of this special trust in their armed forces. Military leaders will have to understand and appreciate the implications associated with unconstrained access to this information.

Leadership Challenges of managing an integrated system

During the Strategic Leadership module, U.S. Army War College students examine the areas of responsible command, leadership, and management practices. A portion of this module centers on the concept of environmental scanning; the idea that by proactively examining current trends a leader can anticipate where his organization will be 10 to 20 years into the future. The application of biometrics as a security

measure is quickly taking root within DoD. One of the best examples of biometrics in use today is the Common Access Card (CAC). In addition to serving as a visual validation of the card holder, it also contains embedded biometrics and a person specific PIN. The point of this example is to illustrate that this is just the beginning of the revolution in security. The real challenge to military leaders in the next two decades will be to develop sophisticated risk management techniques, build up defenses against terrorism, strengthen the borders, sea, and airports, and improve the use and sharing of information technology among government agencies.[26]

Senior military and civilian leaders in this U.S. Army War College class will most likely be at the forefront of this technological revolution in security. The foundations are already being laid and it will be up to us to bring the leadership, talent, and moral fortitude that will be required and expected. As we've experienced, terrorism is already on our soil. Counterterrorism actions around the globe will not stop terrorists from striking the homeland; those efforts will only delay the inevitable -- IEDs on our highways, byways, and streets. The terrorists' ultimate goal is to destroy the American way of life; the military leaders' responsibility is to preserve that way of life, which is no small task. But the ethical and effective use of biometrics as way to combat international terrorism will perhaps help tip the balance in our favor.

Conclusions

The last decade has witnessed the emergence of practical applications of biometrics; or as our own DoD calls it, the Revolution in Security. Already biometrics based security systems are in use on battlefields in Iraq and in Afghanistan, and in many parts of the government and in Corporate America. As this technology takes hold

and gains widespread use, the challenge to military leaders entrusted with safeguarding the identity of millions of our citizens will be to protect that data from potential misuse while still allowing the citizens the benefits of this technology without surrendering their liberty or privacy. Utilization of this technology for purposes of protecting the Homeland will become an even greater focus of the military leadership. Terrorists are a thinking, complex, and adaptive enemy; they will not stop at the borders. Leaders at the forefront of this long war will be challenged at every turn to anticipate enemy actions. The effective use of biometric sciences, coupled with other counterterrorism measures, will be the new first line of defense against the extremist's unrelenting assault on the American way of life.

Recommendations

The emphasis of this research has been on identifying emerging biometrics technologies that are already, or will soon be, sufficiently matured that they can be incorporated into a viable and integrated National Biometrics System. While DoD and the FBI continue to make progress towards fully integrating their existing biometric identification systems, DHS, DOJ, and other Federal Agencies lag behind in focus and direction. The plethora of systems in the various stages of development and implementation today work effectively in their narrow employment focus, but all these methods are largely still stove piped either by agency or by role and/or mission. The central issue is that multiple biometric collection systems and tools are currently being used in the various theaters of operation by different [Federal] agencies and international organizations.[27]

Notwithstanding the unique deployment and coordination hurdles, biometrics technologies have proven their worth when used in combination with integrated security systems. I recommend a focused national effort to consolidate all existing national biometric systems under an integrated master biometrics organization. This should be a long term program commitment that could perhaps span 12 – 15 years. In scope, and no less important, this effort could rival the Apollo program. The project should be planned with a tree tiered approach. The first phase should be to identify, categorize, and compare capabilities and limitations of experimental and currently deployed biometric systems, not only in the government but also in Corporate America. The second phase should focus on developing or adopting technologies that will enable the interoperability of existing designs capitalizing on the strengths and effective features of each. Finally, the third phase of the program should focus on consolidating all national biometric resources into a single, master integrated repertoire of biometric data. This last phase would be the most technologically challenging and potentially the most sensitive, not only in terms of privacy security issues, as discussed above, but also in terms of costs and resources needed to execute. A project of this scope could conceivably cost billions of dollars and at least seven years to complete. The 9/11 Commission Report recommended “the President should lead [a] government-wide effort to bring the major national security institutions into the information revolution. He should coordinate the resolution of the legal, policy and the technical issues across agencies to create a trusted information network.”[28] Without a national commitment of resources to secure our borders, determined radical jihadist terrorists will strike us again, and the next event will dwarf the experience of September 11, 2001.

Endnotes

[1] *Forensic Science - The Crime Fighter's Weapon*, Season 1, Episode 26, 50 min., The History Channel: Modern Marvels, 28 September 1997, DVD.

[2] "Biometrics," *World of Forensic Science,* 2006 [journal on-line]; available from http://www.enotes.com/forensic-science/biometrics.html; Internet; accessed 12 October 2007.

[3] U.S. Department of the Army, *Biometrics Task Force, DoD ABIS*, Trifold (Washington, D.C.: U.S. Department of the Army, April 2007), current initiatives section.

[4] Guy Gugliotta, "The Eyes Have It: Body Scans at the ATM," *Washington Post*, 21 June 1999 [newspaper on-line]; available from http://www.washingtonpost.com/wp-srv/national/daily/june99/scans21.htm; Internet; accessed 12 October 2007.

[5] IBM Corporation, *Effectively manage access to systems and information to help optimize integrity and facilitate compliance,* White Paper (Somers, N.Y.: IBM Governance and Risk Management, March 2007); available from http://www35.ibm.com/services/us /iss/pdf/access_white_paper.pdf; Internet; accessed 11 October 2007.

[6] Systems and Network Analysis Center for Information Assurance, "Biometrics Security Considerations," available from www.nsa.gov/snac; Internet; accessed 12 October 2007.

[7] Arun A. Ross, Karthic Nandhumar and Anil K. Jain, *Handbook of Biometrics* (New York: Springer, 2006), 21.

[8] Lim Dong-hum, "Biometrics as a new technology– Identifying oneself by using unique human characteristics," *The Argus, Theory and Critique*, 1 June 1999 [journal on-line]; available from http://maincc.hufs.ac.kr/~argus/no343/t_c2.htm; Internet; accessed 25 January 2008.

[9] National Center for State Courts, "Individual Biometrics," 2002, available from http://ctl.ncsc.dni.us/biometrics/BMRetinal.html; Internet; accessed 25 January 2008.

[10] Dong-hum.

[11] Ibid.

[12] Ibid.

[13] "Semi Independent Shifting Techniques for Signature Verification," United States Patent #4553259; available from http://freepatensonline.com/455323259.htm; Internet; accessed 12 October 2007.

[14] Dong-hum,

[15] How Stuff Works, "What is a smart card?," http://computer.howstuffworks.com/question332.htm; Internet; accessed 4 January 2008.

[16] *Clear: How Clear Works*, Phamplet (New York: Clear: Fly Through Airport Security, undated); "Fly Through Airport Security,"; available from http://flyclear.com/about/clear _howclearworks.html; Internet; accessed 4 January 2008.

[17] Ross, Nandhumar and Jain, 33.

[18] Ibid.

[19] Defense Science Board, *Report of the Defense Science Board Task Force on Defense Biometrics* (Washington, D.C.: Defense Science Board, Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, March 2007), 11.

[20] U.S. Department of the Army, *Biometrics Task Force, DoD ABIS*, Trifold.

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] Defense Science Board, *Report of the Defense Science Board Task Force on Defense Biometrics*, 70.

[25] Ibid., 73.

[26] Chris Israel, Deputy Assistant Secretary for Technology Policy, U.S. Department of Commerce, "The Security Race: Challenges, Leadership and Tools for Success," 20 May 2002, available from http://www.technology.gov/Speeches/CI_020520_SecurityRace.htm; Internet; accessed 12 October 2007.

[27] Major Charles Seifert and Craig Archer, "USSOCOM Tiger Team Studies Battlefield Biometrics Technology," *Tip of the Spear* (December 2007): 17.

[28] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, D.C.: National Commission on Terrorist Attacks upon the United States, August 2004), 418.